

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 Subject premises and person, more fully described in
 Attachment A

Case No. **MJ21-450**

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Subject premises and person, more fully described in Attachment A

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252(a)(2)	Receipt/Distribution of Child Pornography
18 U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:

- ☒ See Affidavit of Kaylee Johnson, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.



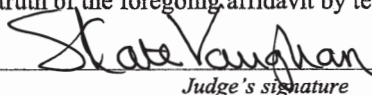
Applicant's signature

SA Kaylee Johnson, FBI

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 08/04/2021



Judge's signature

City and state: Seattle, Washington

S. Kate Vaughan, United States Magistrate Judge

Printed name and title

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

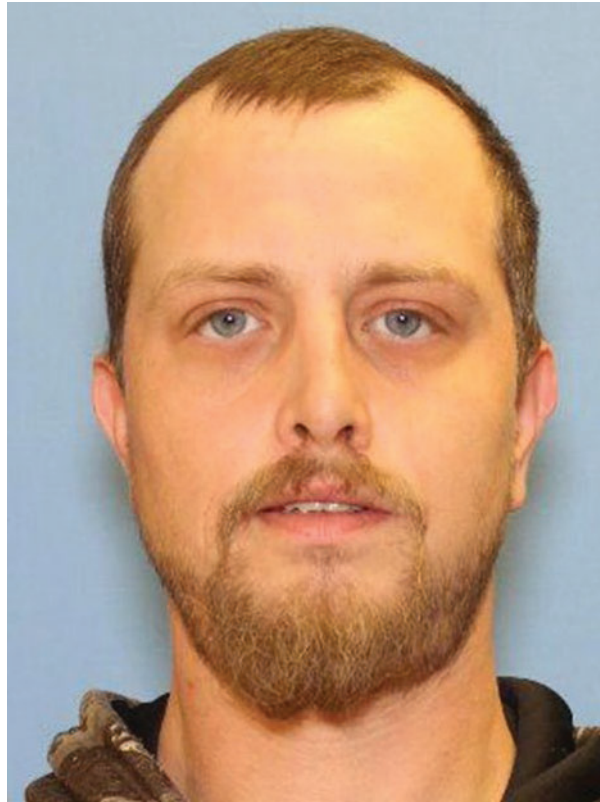
The SUBJECT PREMISES is the property located at 10630 NE 138th Pl. Kirkland, Washington 98034, and is a property containing a two-story, single-family home with blue siding and white trim.



The search is to include the entirety of the residence and all vehicles, garages, attached or detached, or other outbuildings located on the SUBJECT PREMISES, and any digital device(s) found therein.

However, to the extent law enforcement can reasonably determine onsite that the SUBJECT PERSON neither owns nor has access to a particular digital device, this warrant **DOES NOT** authorize its search or seizure.

(PERSON TO BE SEARCHED)



The SUBJECT PERSON is SHAWN DYLAN LEWIS, a white male, 5 feet 10 inches tall, approximately 210 pounds with blue eyes, and brown hair.

The search is to include the SUBJECT PERSON and any backpacks, bags, or other containers that SUBJECT PERSON may be carrying, as well as any digital devices(s) or other electronic storage media found on the SUBJECT PERSON or therein.

ATTACHMENT B**ITEMS TO BE SEIZED**

Evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt/Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) committed in or after January 2019:

- a. Items, records, or information³ relating to visual depictions of minors engaged in sexually explicit conduct;
- b. Items, records, or information relating to the use of the Kik Network;
- c. Items, records, or information relating to the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;
- d. Items, records, or information concerning communications about the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;
- e. Items, records, or information concerning communications about the sexual abuse or exploitation of minors;
- f. Items, records, or information related to communications with or about minors;
- g. Items, records, or information concerning the identities and contact information (including mailing addresses) of any individuals involved in the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct, saved in any form;
- h. Items, records, or information concerning occupancy, residency or ownership of the SUBJECT PREMISES, including without limitation,

³ As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

1 utility and telephone bills, mail envelopes, addressed correspondence,
 2 purchase or lease agreements, diaries, statements, identification documents,
 3 address books, telephone directories, and keys;

4 i. Items, records, or information concerning the ownership or use of computer
 5 equipment found in the SUBJECT PREMISES, including, but not limited
 6 to, sales receipts, bills for internet access, handwritten notes, and computer
 7 manuals;

8 j. Any digital devices or other electronic storage media⁴ and/or their
 9 components including:

10 i. any digital device or other electronic storage media capable of being
 11 used to commit, further, or store evidence, fruits, or instrumentalities
 12 of the offenses listed above;

13 ii. any magnetic, electronic or optical storage device capable of storing
 14 data, including thumb drives, SD cards, or external hard drives;

15 iii. any physical keys, encryption devices, dongles and similar physical
 16 items that are necessary to gain access to the computer equipment,
 17 storage devices or data; and

18 iv. any passwords, password files, test keys, encryption codes or other
 19 information necessary to access the computer equipment, storage
 20 devices or data.

21 k. For any digital device or other electronic storage media whose seizure is
 22 otherwise authorized by this warrant, and any digital device or other
 23 electronic storage media that contains or in which is stored records or
 24 information that is otherwise called for by this warrant:

25 i. evidence of who used, owned, or controlled the digital device or
 26 other electronic storage media at the time the things described in this
 27 warrant were created, edited, or deleted, such as logs, registry
 28

26 ⁴ The term “digital devices” includes all types of electronic, magnetic, optical, electrochemical,
 27 or other high speed data processing devices performing logical, arithmetic, or storage functions,
 28 including desktop computers, notebook computers, mobile phones, tablets, server computers, and
 network hardware. The term “electronic storage media” includes any physical object upon
 which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash
 memory, CD-ROMs, and other magnetic or optical media.

1 entries, configuration files, saved usernames and passwords,
2 documents, browsing history, user profiles, email, email contacts,
3 “chat,” instant messaging logs, photographs, and correspondence;

4 ii. evidence of software that would allow others to control the digital
5 device or other electronic storage media, such as viruses, Trojan
6 horses, and other forms of malicious software, as well as evidence of
7 the presence or absence of security software designed to detect
8 malicious software;

9 iii. evidence of the lack of such malicious software;

10 iv. evidence of the attachment to the digital device of other storage
11 devices or similar containers for electronic evidence;

12 v. evidence of counter-forensic programs (and associated data) that are
13 designed to eliminate data from the digital device or other electronic
14 storage media;

15 vi. evidence of the times the digital device or other electronic storage
16 media was used;

17 vii. passwords, encryption keys, and other access devices that may be
18 necessary to access the digital device or other electronic storage
19 media;

20 viii. documentation and manuals that may be necessary to access the
21 digital device or other electronic storage media or to conduct a
22 forensic examination of the digital device or other electronic storage
23 media;

24 ix. records of or information about the Internet Protocol used by the
25 digital device or other electronic storage media;

26 x. records of internet activity, including firewall logs, caches, browser
27 history and cookies, “bookmarked” or “favorite” web pages, search
28 terms that the user entered into any internet search engine, and
records of user-typed web addresses.

xi. contextual information necessary to understand the evidence
described in this attachment.

1 This warrant authorizes a review of electronic storage media and electronically stored
2 information seized or copied pursuant to this warrant in order to locate evidence, fruits,
3 and instrumentalities described in this warrant. The review of this electronic data may be
4 conducted by any government personnel assisting in the investigation, who may include,
5 in addition to law enforcement officers and agents, attorneys for the government, attorney
6 support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a
7 complete copy of the seized or copied electronic data to the custody and control of
8 attorneys for the government and their support staff for their independent review.

9 THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE
10 MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS
11 SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO
12 THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC
13 STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL
14 ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE
15 CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR
16 EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED
17 CRIMES.
18
19
20
21
22
23
24
25
26
27
28

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Kaylee Johnson, having been duly sworn, state as follows:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), currently assigned to the Seattle Division. I have been employed as an FBI Special Agent since 2020. I am responsible for investigations involving Violent Crimes Against Children, which includes sex trafficking of minors, occurring in the Western District of Washington. My duties as a Special Agent include the enforcement of federal criminal statutes involving the sexual exploitation of children pursuant to Title 18, United States Code, Sections 2251 through 2259, and Sections 1591 through 1592. I specialize in the area of child sexual exploitation, and have had the opportunity to review numerous examples of child pornography (as defined in Title 18, United States Code, Section 2256) in all forms of media, including computer media. I am a member of the Seattle Internet Crimes Against Children (ICAC) Task Force in the Western District of Washington, and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children. I have participated in multiple child pornography investigations, and I have received training regarding Internet crimes and child exploitation investigations. I have participated in the execution of search warrants which involved child exploitation and/or child pornography offenses and the search and seizure of computers and other digital devices. Further, I have served as the affiant on search warrants relating to child exploitation investigations.

2. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this

1 investigation, including other law enforcement officers; review of documents and records
2 related to this investigation; communications with others who have personal knowledge
3 of the events and circumstances described herein; and information gained through my
4 training and experience.

5 **PURPOSE OF THE AFFIDAVIT**

6 3. I make this affidavit in support of an application under Rule 41 of the
7 Federal Rules of Criminal Procedure for search warrants for the following location and
8 persons:

9 (1) The premises located at 10630 NE 138th Pl. Kirkland, WA 98034 (hereinafter
10 the "SUBJECT PREMISES"), further described in Attachment A, which is
11 incorporated herein by reference; and

12 (2) The person of SHAWN DYLAN LEWIS (hereinafter the "SUBJECT
13 PERSON," further described in Attachment A, which is incorporated herein by
14 reference.

15 4. As set forth below, there is probable cause to believe the SUBJECT
16 PERSON resides at the SUBJECT PREMISES and engaged in online chats about and
17 exchanged material depicting the sexual abuse of children. There is, therefore, probable
18 cause to believe that the SUBJECT PREMISES and SUBJECT PERSON will contain
19 evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. § 2252(a)(2)
20 (Receipt/Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession
21 of Child Pornography), the TARGET OFFENSES. I seek authorization to search and
22 seize the items specified in Attachment B.

23 5. The information in this affidavit is based upon the investigation I have
24 conducted in this case, my conversations with other law enforcement officers who have
25 engaged in various aspects of this investigation, and my review of reports written by
26 other law enforcement officers involved in this investigation. Because this affidavit is
27 being submitted for the limited purpose of securing search warrants, I have not included
28 each and every fact known to me concerning this investigation. I have set forth only

1 those facts that I believe are sufficient to establish probable cause to support the issuance
2 of the requested warrants. When the statements of others are set forth in this affidavit,
3 they are set forth in substance and in part.

4 6. This Affidavit is being presented electronically pursuant to Local Criminal
5 Rule CrR 41(d)(3).

6 **BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE**

7 7. In February 2021, an FBI online covert employee (“OCE”), working in an
8 uncover capacity, saw a Kik user distribute child sexual abuse material (CSAM) using the
9 Kik platform. Kik is a smartphone messenger application that allows users to send text
10 messages, photos, and videos to other users in either a private, one-on-one conversation
11 or in a group conversation with multiple users. Kik is used primarily on smartphones and
12 tablets. The Kik app is available for free on both the Android and iOS platforms.

13 8. During an undercover session on or about February 19, 2021, the OCE saw
14 the Kik user jordan022380 (hereinafter referred to as the SUBJECT USER) with the
15 display name “Jordan L,” distribute suspected CSAM.

16 9. The OCE created a copy of the conversation with the SUBJECT USER on
17 Kik and copied the two videos sent by the SUBJECT USER. The OCE sent this
18 information, along with other information gathered in the OCE’s investigation, in an
19 investigative referral to Seattle FBI.

20 10. On June 14, 2021, I received a disc containing the conversation between the
21 SUBJECT USER and OCE, as well as the two videos sent by the SUBJECT USER
22 during the conversation. I reviewed the messages sent from the SUBJECT USER and
23 OCE. During one conversation, the OCE asked the SUBJECT USER, “You into young?”
24 The SUBJECT USER responded, “Yeah”. The OCE responded, “Nice. How young?”
25 The SUBJECT user responded, “Any” and “No limits”. In the chat, I saw that the
26 SUBJECT USER asked “You a dad,” to which the OCE replied “Yup. U?” The
27 SUBJECT USER replied “Yeah,” “How old,” and the OCE replied “11”. The SUBJECT
28 USER stated “Nice” and “Mine is 12”. The OCE asked the SUBJECT USER “we’re you

1 and your daughter active before?” and the SUBJECT USER replied “I started to touch
2 her”.

3 11. During the review of the messages, I saw that the SUBJECT USER sent a
4 video (File 1) on February 19, 2021, at 8:29:59 PM(UTC+0) and a second video (File 2)
5 sent on February 19, 2021, at 8:37:45PM(UTC+0).

6 12. On June 14, 2021, I reviewed the two videos sent by the SUBJECT USER
7 to the OCE as described below:

8 **File 1-**

9 This video, approximately 43 seconds long, depicts one prepubescent female who is fully
10 nude. In the video, the child victim states, “do you like it? Maybe some pictures in the
11 mirror?” The child victim uses her fingers to touch her vagina. Based upon the small
12 stature, lack of breast development, lack of muscular development, facial features, voice,
13 and lack of body development, I estimate that the child victim is approximately 8-11
14 years of age.

15 **File 2-**

16 This video, approximately 21 seconds long, depicts a female who is dressed. The video
17 shows the female undress in front of the camera until she is fully nude. The angle in the
18 video does not give a view of the female’s face. I was unable to determine whether the
19 female is a minor.

20 13. In response to an administrative summons sent by SA Burns seeking
21 subscriber information for the Kik user jordan022380, Kik reported that the SUBJECT
22 USER used IP address 24.16.29.1 (SUBJECT IP ADDRESS) on multiple occasions
23 between January 31, and March 1, 2021, to connect to Kik servers. Specifically, the
24 SUBJECT USER used the SUBJECT IP ADDRESS to connect to Kik’s servers on
25 February 19, 2021, the date that the SUBJECT USER distributed the two videos
26 described above. Kik also reported the SUBJECT USER provided an unconfirmed email
27 address of ironboy8401@yahoo.com and had registered the account using a Samsung
28 device.

14. A query of a publicly available database revealed that the SUBJECT IP
ADDRESS belonged to Comcast. In response to an administrative subpoena seeking
subscriber information for the SUBJECT IP ADDRESS, Comcast reported that the

1 SUBJECT IP ADDRESS was assigned to Terry Shaw with a service address at the
2 SUBJECT PREMISES from January 31, 2021, through March 1, 2021.

3 15. I also learned that in 2019, FBI Indianapolis identified another Kik user,
4 ironboy8401, associated with the SUBJECT IP ADDRESS who distributed suspected
5 CSAM over Kik. As part of that investigation, FBI Indianapolis obtained chat logs
6 between the user ironboy8401 and their subject. I obtained and reviewed copies of these
7 chats. Notably, the user ironboy8401's display name in these chats was "ironboy8401
8 Dylan ;)."

9 16. During the conversation, ironboy8401 said, "Wish I was at home alone
10 with the daughter," to which other Kik user replied, "Same". User ironboy8401 asked if
11 the other user got "any good pics yesterday," to which the other user replied, "I didn't
12 sadly, I got a bit nervous about it haha". User ironboy8401 responded, "Don't blame
13 you". The other user then said, "I know I'm VERY into this stuff (also I don't think I
14 answered your question about other stuff I'm into but mostly you name it I love it) but I
15 feel bad sometimes and phase out a bit lol," and ironboy8401 responded, "I feel you
16 there". The other user then said, "That's good to know :)" and ironboy8401 replied,
17 "Yeah". User ironboy8401 then sent the image described below, which I reviewed:

18 **File 1-**

19 This photo depicted a prepubescent female sitting in the front seat of a vehicle with her
20 genitals exposed to the camera. Based upon the small stature, facial features, and the lack
21 of muscular development, I estimate the child victim is approximately 3-5 years old.

22 17. In response to an administrative subpoena seeking subscriber information
23 for ironboy8401, Kik reported the following information:

24 First Name: Dylan

25 Last Name: ;)

26 Email address: ironboy223@gmail.com (confirmed)

27 18. Kik also provided IP connection information showing that the SUBJECT IP
28 ADDRESS was among the IP addresses ironboy8401 used to connect to Kik's servers

1 between September 1, and September 30, 2019. In response to an administrative
2 subpoena, Comcast reported that the SUBJECT IP ADDRESS was assigned to Terry
3 Shaw with a service address at the at the SUBJECT PREMISES between September 1,
4 and September 30, 2019.

5 19. FBI Indianapolis located an Instagram account associated with the email
6 address ironboy223@gmail.com. The Instagram account had a username of “ironboy223”
7 and a profile name of “Dylan Lewis.” FBI also located a Facebook profile with the
8 Facebook User ID of facebook.com/dylan.lewis.129. Among the publicly available
9 photos associated with that account was a photo identical to the publicly available profile
10 photos on the above Instagram account. That photo depicts an adult male who looks to
11 be the same person depicted in Washington driver license photo I obtained for the
12 SUBJECT PERSON.

13 I reviewed other publicly available information associated with the
14 Dylan.lewis.129 Facebook account. The Facebook page had the username “Dylan
15 Lewis” and had a status from June 13, 2021 stating this user was “In a Relationship with
16 Misty Shaw.” I located a Facebook profile for “Misty Shaw,” which has a post from July
17 2016 indicating she is in a relationship with “Dylan Lewis.”

18 20. Washington DOL information shows that the SUBJECT PERSON has a
19 valid Washington driver’s license issued in 2017 that lists a residential address in
20 Woodinville, Washington. However, open source searches of publicly available
21 information show that the SUBJECT PERSON has been associated with the SUBJECT
22 PREMISES since January 2019. While conducting surveillance at the SUBJECT
23 PREMISES on July 7, 2021, I saw a white Acura park at the residence at approximately
24 2:00 p.m. I saw a white male, whom I positively identified as the SUBJECT PERSON,
25 get out of the car and enter the residence. This car, bearing the Washington license plate
26 number BVA0492, is registered to the SUBJECT PERSON at the SUBJECT PREMISES.

27 21. From my investigation, I believe that the SUBJECT PERSON currently
28 resides at the SUBJECT PREMISES and has resided there since at least 2019. From my

1 investigation, I believe that four other adults may also reside at the SUBJECT
2 PREMISES: Byron Vincent Shaw, Terry Vincent Shaw, Cynthia Shaw, and Misty Shaw.
3 One or more minors may reside at the SUBJECT PREMISES as well.

4 22. I know from my training and experience that users of Kik Messenger
5 generally do not share Kik accounts with one another. Because of the nature of how Kik
6 Messenger works, it would be difficult to do so effectively. More specifically, each time
7 a user logs into Kik Messenger on a device, the content associated with that user's
8 account will be removed from any other device from which that user logged into the
9 account. So, while it is theoretically possible that multiple persons could use the same
10 Kik Messenger account over a period of time, that would be unusual. Due to the IP
11 Address that was in use on February 19, 2021, I believe it is likely the SUBJECT
12 PERSON is the SUBJECT USER and is the person responsible for the SUBJECT
13 USER's activity on Kik Messenger described above.

14 **BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY**

15 23. I have had both training and experience in the investigation of computer-
16 related crimes. Based on my training, experience, and knowledge, I know the following:

17 a. Computers and digital technology are the primary way in which
18 individuals interested in child pornography interact with each other. Computers basically
19 serve four functions in connection with child pornography: production, communication,
20 distribution, and storage.

21 b. Digital cameras and smartphones with cameras save photographs or
22 videos as a digital file that can be directly transferred to a computer by connecting the
23 camera or smartphone to the computer, using a cable or via wireless connections such as
24 "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may
25 be stored on a removable memory card in the camera or smartphone. These memory
26 cards are often large enough to store thousands of high-resolution photographs or videos.

27 c. A device known as a modem allows any computer to connect to
28 another computer through the use of telephone, cable, or wireless connection. Mobile
29 devices such as smartphones and tablet computers may also connect to other computers
30 via wireless connections. Electronic contact can be made to literally millions of
31 computers around the world. Child pornography can therefore be easily, inexpensively
32 and anonymously (through electronic communications) produced, distributed, and
33 received by anyone with access to a computer or smartphone.

1 d. The computer's ability to store images in digital form makes the
2 computer itself an ideal repository for child pornography. Electronic storage media of
3 various types - to include computer hard drives, external hard drives, CDs, DVDs, and
4 "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a
5 port on the computer - can store thousands of images or videos at very high resolution. It
6 is extremely easy for an individual to take a photo or a video with a digital camera or
7 camera-bearing smartphone, upload that photo or video to a computer, and then copy it
8 (or any other files on the computer) to any one of those media storage devices. Some
9 media storage devices can easily be concealed and carried on an individual's person.
10 Smartphones and/or mobile phones are also often carried on an individual's person.

11 e. The Internet affords individuals several different venues for
12 obtaining, viewing, and trading child pornography in a relatively secure and anonymous
13 fashion.

14 f. Individuals also use online resources to retrieve and store child
15 pornography. Some online services allow a user to set up an account with a remote
16 computing service that may provide email services and/or electronic storage of computer
17 files in any variety of formats. A user can set up an online storage account (sometimes
18 referred to as "cloud" storage) from any computer or smartphone with access to the
19 Internet. Even in cases where online storage is used, however, evidence of child
20 pornography can be found on the user's computer, smartphone, or external media in most
21 cases.

22 g. A growing phenomenon related to smartphones and other mobile
23 computing devices is the use of mobile applications, also referred to as "apps." Apps
24 consist of software downloaded onto mobile devices that enable users to perform a
25 variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or
26 playing a game – on a mobile device. Individuals commonly use such apps to receive,
27 store, distribute, and advertise child pornography, to interact directly with other like-
28 minded offenders or with potential minor victims, and to access cloud-storage services
where child pornography may be stored.

1 h. As is the case with most digital technology, communications by way
2 of computer can be saved or stored on the computer used for these purposes. Storing this
3 information can be intentional (i.e., by saving an email as a file on the computer or saving
4 the location of one's favorite websites in, for example, "bookmarked" files) or
5 unintentional. Digital information, such as the traces of the path of an electronic
6 communication, may also be automatically stored in many places (e.g., temporary files or
7 ISP client software, among others). In addition to electronic communications, a
8 computer user's Internet activities generally leave traces or "footprints" in the web cache
9 and history files of the browser used. Such information is often maintained indefinitely
10 until overwritten by other

11 24. Based upon my knowledge, experience, and training in child pornography
12 investigations, and the training and experience of other law enforcement officers with
13 whom I have had discussions, I know that there are certain characteristics common to
14 individuals who have a sexualized interest in children and depictions of children:

15 a. They may receive sexual gratification, stimulation, and satisfaction
16 from contact with children; or from fantasies they may have viewing children engaged in
17 sexual activity or in sexually suggestive poses, such as in person, in photographs, or other
18 visual media; or from literature describing such activity.

19 b. They may collect sexually explicit or suggestive materials in a
20 variety of media, including photographs, magazines, motion pictures, videotapes, books,
21 slides, and/or drawings or other visual media. Such individuals often times use these
22 materials for their own sexual arousal and gratification. Further, they may use these
23 materials to lower the inhibitions of children they are attempting to seduce, to arouse the
24 selected child partner, or to demonstrate the desired sexual acts. These individuals may
25 keep records, to include names, contact information, and/or dates of these interactions, of
26 the children they have attempted to seduce, arouse, or with whom they have engaged in
27 the desired sexual acts.

28 c. They often maintain any "hard copies" of child pornographic
material that is, their pictures, films, video tapes, magazines, negatives, photographs,
correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of
their home or some other secure location. These individuals typically retain these "hard
copies" of child pornographic material for many years, as they are highly valued.

 d. Likewise, they often maintain their child pornography collections
that are in a digital or electronic format in a safe, secure and private environment, such as
a computer and surrounding area. These collections are often maintained for several
years and are kept close by, often at the individual's residence or some otherwise easily
accessible location, to enable the owner to view the collection, which is valued highly.

1 e. They also may correspond with and/or meet others to share
2 information and materials; rarely destroy correspondence from other child pornography
3 distributors/collectors; conceal such correspondence as they do their sexually explicit
4 material; and often maintain lists of names, addresses, and telephone numbers of
5 individuals with whom they have been in contact and who share the same interests in
6 child pornography.

7 f. They generally prefer not to be without their child pornography for
8 any prolonged time period. This behavior has been documented by law enforcement
9 officers involved in the investigation of child pornography throughout the world.
10 Importantly, e-mail and cloud storage can be a convenient means by which individuals
11 can access a collection of child pornography from any computer, at any location with
12 Internet access. Such individuals therefore do not need to physically carry their
13 collections with them but rather can access them electronically. Furthermore, these
14 collections can be stored on email "cloud" servers, which allow users to store a large
15 amount of material at no cost, and possibly reducing the amount of any evidence of any
16 of that material on the users' computer(s).

17 25. Even if such individuals use a portable device (such as a mobile phone) to
18 access the Internet and child pornography, it is more likely than not that evidence of this
19 access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment
20 A, including on digital devices other than the portable device (for reasons including the
21 frequency of "backing up" or "synching" mobile phones to computers or other digital
22 devices).

23 26. In addition to offenders who collect and store child pornography, law
24 enforcement has encountered offenders who obtain child pornography from the internet,
25 view the contents and subsequently delete the contraband, often after engaging in self-
26 gratification. In light of technological advancements, increasing Internet speeds and
27 worldwide availability of child sexual exploitative material, this phenomenon offers the
28 offender a sense of decreasing risk of being identified and/or apprehended with quantities
of contraband. This type of consumer is commonly referred to as a 'seek and delete'
offender, knowing that the same or different contraband satisfying their interests remain
easily discoverable and accessible online for future viewing and self-gratification. I
know that, regardless of whether a person discards or collects child pornography he/she
accesses for purposes of viewing and sexual gratification, evidence of such activity is

likely to be found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

27. Given the above-stated facts and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe that the SUBJECT PERSON is the SUBJECT USER and likely has a sexualized interest in children and depictions of children, and that evidence of the commission of the TARGET OFFENSES is therefore likely to be found at the SUBJECT PREMISES or on the SUBJECT PERSON.

FRUITS, EVIDENCE, AND INSTRUMENTALITIES INSIDE THE SUBJECT PREMISES/ON THE SUBJECT PERSON AND ANY CLOSED CONTAINERS AND ELECTRONIC DEVICES FOUND THEREIN

28. As described above and in Attachment B, this application seeks permission to search for and seize items listed in Attachment B that might be found in the SUBJECT PREMISES or on the SUBJECT PERSON, in whatever form they are found. One form in which evidence, fruits, or instrumentalities might be found is data stored on a computer's hard drive or other digital device¹ or electronic storage media.² Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

¹ "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

² Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

29. Through my training and experience, and the information learned during the course of this investigation, I know that individuals who engage in child pornography offenses often keep physical evidence, fruits, and instrumentalities of their crimes inside their residences, including but not limited to, digital devices

30. *Probable cause.* Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensic examiners, and my training and experience, I submit that if a digital device or other electronic storage medium is found in the SUBJECT PREMISES or on the SUBJECT PERSON, there is probable cause to believe that evidence, fruits, and instrumentalities of the TARGET OFFENSES will be stored on those digital devices or other electronic storage media. As noted above, my investigation has shown that the SUBJECT PERSON resides at the SUBJECT PREMISES and, among other things, used a digital device to connect to Kik Messenger and uploaded visual depictions of minors/a minor engaged in sexually explicit conduct. There is, therefore, probable cause to believe that evidence, fruits, and instrumentalities, of the crimes under investigation exist and will be found on digital devices or other electronic storage media at the SUBJECT PREMISES or on the SUBJECT PERSON for at least the following reasons:

a. Based my knowledge, training, and experience, I know that computer files or remnants of such files may be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, this information can sometimes be recovered months or years later with forensics tools. This is because when a person “deletes” a file on a computer, the data contained in the files does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in “swap” or “recovery” files.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a

1 computer has been used, what is has been used for, and who has used it. To give a few
 2 examples, this forensic evidence can take the form of operating system configurations,
 3 artifacts from operating system or application operation, file system data structures, and
 4 virtual memory “swap” paging files. Computer users typically do not erase or delete this
 evidence, because special software is typically required for that task. However, it is
 technically possible to delete this information.

5
 6 d. Similarly, files that have been viewed via the Internet are sometimes
 automatically downloaded into a temporary Internet directory or “cache.”

7
 8 e. Digital storage devices may also be large in capacity, but small in
 9 physical size. Because those who are in possession of such devices also tend to keep
 10 them on their persons, especially when they may contain evidence of a crime. Digital
 storage devices may be smaller than a postal stamp in size, and thus they may easily be
 hidden in a person’s pocket.

11 31. As further described in Attachment B, this application seeks permission to
 12 locate not only computer files that might serve as direct evidence of the crimes described
 13 on the warrant, but also for forensic electronic evidence that establishes how computers
 14 were used, the purpose of their use, who used them, and when. There is probable cause
 15 to believe that this forensic electronic evidence will be on digital devices found in the
 16 SUBJECT PREMISES or on the SUBJECT PERSON because:

17
 18 a. Data on the digital storage medium or digital devices can provide
 19 evidence of a file that was once on the digital storage medium or digital devices but has
 20 since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has
 21 been deleted from a word processing file). Virtual memory paging systems can leave
 22 traces of information on the storage medium that show what tasks and processes were
 23 recently active. Web browsers, e-mail programs, and chat programs store configuration
 24 information on the storage medium that can reveal information such as online nicknames
 25 and passwords. Operating systems can record additional information, such as the
 attachment of peripherals, the attachment of USB flash storage devices or other external
 storage media, and the times the computer was in use. Computer file systems can record
 information about the dates files were created and the sequence in which they were
 created, although this information can later be falsified.

26
 27 b. As explained herein, information stored within a computer and other
 28 electronic storage media may provide crucial evidence of the “who, what, why, when,
 where, and how” of the criminal conduct under investigation, thus enabling the United
 States to further establish and prove each element or alternatively, to exclude the innocent

1 from further suspicion. In my training and experience, information stored within a
2 computer or storage media (e.g. registry information, communications, images and
3 movies, transactional information, records of session times and durations, Internet
4 history, and anti-virus, spyware, and malware detection programs) can indicate who has
5 used or controlled the computer or storage media. This “user attribution” evidence is
6 analogous to the search of “indicia of occupancy” while executing a search warrant at a
7 residence. The existence or absence of anti-virus, spyware, and malware detection
8 programs may indicate whether the computer was remotely accessed, thus inculcating or
9 exculpating the computer owner. Further computer and storage media activity can
10 indicate how and when the computer or storage media was accessed or used. For
11 example, as described herein, computers typically contain information that log computer
12 activity associated with user accounts and electronic storage media that connected with
13 the computer. Such information allows investigators to understand the chronological
14 context of computer or electronic storage media access, use, and events relating to the
15 crime under investigation. Additionally, some information stored within a computer or
16 electronic storage media may provide crucial evidence relating to the physical location of
17 other evidence and the suspect. For example, images stored on a computer may both
18 show a particular location and have geolocation information incorporated into its file
19 data. Such file data typically also contains information indicating when the file or image
20 was created. The existence of such image files, along with external device connection
logs, may also indicate the presence of additional electronic storage media (e.g., a digital
camera or cellular phone with an incorporated camera). The geographic and timeline
information described herein may either inculcate or exculpate the computer user. Last,
information stored within a computer may provide relevant insight into the computer
user’s state of mind as it relates to the offense under investigation. For example,
information within the computer may indicate the owner’s motive and intent to commit
the crime (e.g. Internet searches indicating criminal planning), or consciousness of guilt
(e.g., running a “wiping” program to destroy evidence on the computer or password
protecting/encrypting such evidence in an effort to conceal it from law enforcement).

21 c. A person with appropriate familiarity with how a computer works
22 can, after examining this forensic evidence in its proper content, draw conclusions about
23 how computers were used, the purpose of their use, who used them, and when.

24 d. The process of identifying the exact files, blocks, registry entries,
25 logs, or other forms of forensic evidence on a storage medium that are necessary to draw
26 an accurate conclusion is a dynamic process. While it is possible to specify in advance
27 the records to be sought, computer evidence is not always data that can be merely
28 reviewed by a review team and passed along to investigators. Whether data stored on a
computer is evidence may depend on other information stored on the computer and the
application of knowledge about how a computer behaves. Therefore, contextual
information necessary to understand other evidence also falls within the scope of the
warrant.

1 e. Further, in finding evidence of how a computer was used, the
 2 purpose of its use, who used it, and when, sometimes it is necessary to establish that a
 3 particular thing is not present on a storage medium. For example, the presence or
 4 absence of counter-forensic programs or anti-virus programs (and associated data) may
 be relevant to establishing a user's intent.

5 f. I know that when an individual uses a computer to store, receive, or
 6 distribute child pornography, the individual's computer or digital device will generally
 7 serve both as an instrumentality for committing the crime, and also as a storage medium
 8 for evidence of the crime. The computer or digital device is an instrumentality of the
 9 crime because it is used as a means of committing the criminal offense. The computer or
 10 digital device is also likely to be a storage medium for evidence of crime. From my
 11 training and experience, I believe that a computer or digital device used to commit a
 crime of this type may contain: data that is evidence of how the computer was used; data
 that was sent or received; notes as to how the criminal conduct was achieved; records of
 text discussions about the crime; and other records that indicate the nature of the offense.

12 32. *Necessity of seizing or copying entire computers or storage medium.* In
 13 most cases, a thorough search of a premises for information that might be stored on
 14 digital storage media or other digital devices often requires the seizure of the digital
 15 devices and digital storage media for later off-site review consistent with the warrant. In
 16 lieu of removing storage media from the premises, it is sometimes possible to make an
 17 image copy of storage media. Generally speaking, imaging is the taking of a complete
 18 electronic copy of the digital media's data, including all hidden sectors and deleted files.
 19 Either seizure or imaging is often necessary to ensure the accuracy and completeness of
 20 data recorded on the storage media, and to prevent the loss of the data either from
 21 accidental or intentional destruction. This is true because of the following:

22 a. *The time required for an examination.* As noted above, not all
 23 evidence takes the form of documents and files that can be easily viewed on site.
 24 Analyzing evidence of how a computer has been used, what it has been used for, and who
 25 has used it requires considerable time, and taking that much time on premises could be
 26 unreasonable. As explained above, because the warrant calls for forensic electronic
 27 evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage
 28 media to obtain evidence. Storage media can store a large volume of information.
 Reviewing that information for things described in the warrant can take weeks or months,
 depending on the volume of data stored, and would be impractical and invasive to
 attempt on-site.

1 b. *Technical requirements.* Computers can be configured in several
2 different ways, featuring a variety of different operating systems, application software,
3 and configurations. Therefore, searching them sometimes requires tools or knowledge
4 that might not be present on the search site. The vast array of computer hardware and
5 software available makes it difficult to know before a search what tools or knowledge
6 will be required to analyze the system and its data on-site. However, taking the storage
7 media off-site and reviewing it in a controlled environment will allow its examination
8 with the proper tools and knowledge.

9 c. *Variety of forms of electronic media.* Records sought under this
10 warrant could be stored in a variety of storage media formats that may require off-site
11 reviewing with specialized forensic tools.

12 33. Searching computer systems is a highly technical process that requires
13 specific expertise and specialized equipment. There are so many types of computer
14 hardware and software in use today that it is rarely possible to bring to the search site all
15 the necessary technical manuals and specialized equipment necessary to consult with
16 computer personnel who have expertise in the type of computer, operating system, or
17 software application being searched.

18 34. The analysis of computer systems and storage media often relies on
19 rigorous procedures designed to maintain the integrity of the evidence and to recover
20 “hidden,” mislabeled, deceptively named, erased, compressed, encrypted or password-
21 protected data, while reducing the likelihood of inadvertent or intentional loss or
22 modification of data. A controlled environment such as a laboratory, is typically required
23 to conduct such an analysis properly.

24 35. The volume of data stored on many computer systems and storage devices
25 will typically be so large that it will be highly impracticable to search for data during the
26 execution of the physical search of the premises. The hard drives commonly included in
27 desktop and laptop computers are capable of storing millions of pages of text.

28 36. A search of digital devices for evidence described in Attachment B may
require a range of data analysis techniques. In some cases, agents may recover evidence
with carefully targeted searches to locate evidence without requirement of a manual
search through unrelated materials that may be commingled with criminal evidence.

1 Agents may be able to execute a “keyword” search that searches through the files stored
2 in a digital device for special terms that appear only in the materials covered by the
3 warrant. Or, agents may be able to locate the materials covered by looking for a
4 particular directory or name. However, in other cases, such techniques may not yield the
5 evidence described in the warrant. Individuals may mislabel or hide files and directories;
6 encode communications to avoid using keywords; attempt to delete files to evade
7 detection; or take other steps designed to hide information from law enforcement
8 searches for information.

9 37. The search procedure of any digital device seized may include the
10 following on-site techniques to seize the evidence authorized in Attachment B:

11 a. On-site triage of computer systems to determine what, if any,
12 peripheral devices or digital storage units have been connected to such computer systems,
13 a preliminary scan of image files contained on such systems and digital storage devices to
help identify any other relevant evidence or co-conspirators.

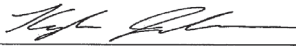
14 b. On-site copying and analysis of volatile memory, which is usually
15 lost if a computer is powered down, and may contain information about how the
16 computer is being used, by whom, when and may contain information about encryption,
virtual machines, or steganography which will be lost if the computer is powered down.

17 c. On-site forensic imaging of any computers may be necessary for
18 computers or devices that may be partially or fully encrypted in order to preserve
19 unencrypted data that may, if not immediately imaged on-scene become encrypted and
20 accordingly become unavailable for any examination.

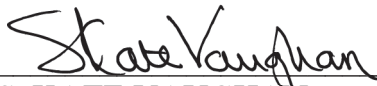
21 38. *Nature of examination.* Based on the foregoing, and consistent with Rule
22 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise
23 copying storage media that reasonably appear to contain some or all of the evidence
24 described in the warrant, and would authorize a later review of the media or information
25 consistent with the warrant. The later review may require techniques, including but not
26 limited to computer-assisted scans of the entire medium, that might expose many parts of
27 a hard drive to human inspection in order to determine whether it is evidence described
28 by the warrant.

CONCLUSION

39. Based on the information set forth herein, there is probable cause to search the above described SUBJECT PREMISES and SUBJECT PERSON, as further described in Attachment A, as well as on and in any digital device or other electronic storage media found at the SUBJECT PREMISES or on the SUBJECT PERSON, for evidence, fruits and instrumentalities, as further described in Attachment B, of the TARGET OFFENSES.


KAYLEE JOHNSON
Special Agent
Federal Bureau of Investigation

The above-named agent provided a sworn statement attesting to the truth of the foregoing Affidavit this o before me this 4th day of August, 2021.


S. KATE VAUGHAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

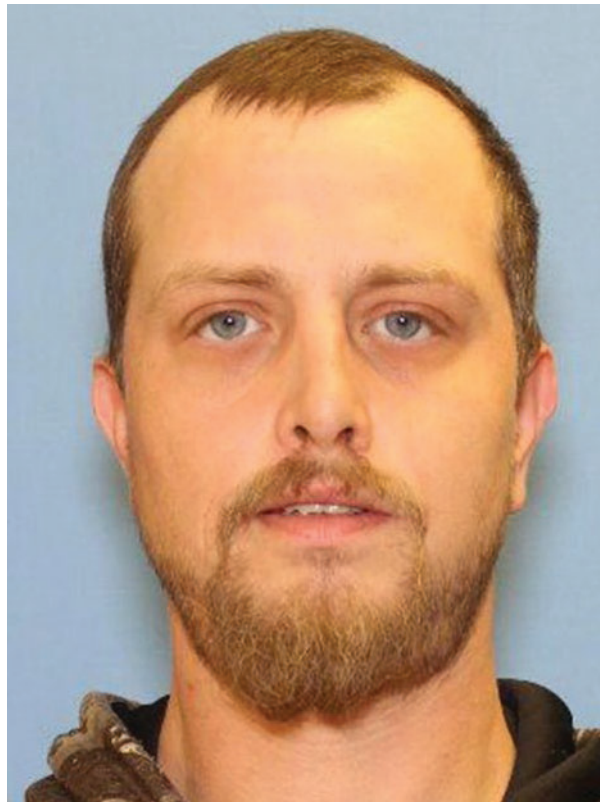
The SUBJECT PREMISES is the property located at 10630 NE 138th Pl. Kirkland, Washington 98034, and is a property containing a two-story, single-family home with blue siding and white trim.



The search is to include the entirety of the residence and all vehicles, garages, attached or detached, or other outbuildings located on the SUBJECT PREMISES, and any digital device(s) found therein.

However, to the extent law enforcement can reasonably determine onsite that the SUBJECT PERSON neither owns nor has access to a particular digital device, this warrant **DOES NOT** authorize its search or seizure.

(PERSON TO BE SEARCHED)



The SUBJECT PERSON is SHAWN DYLAN LEWIS, a white male, 5 feet 10 inches tall, approximately 210 pounds with blue eyes, and brown hair.

The search is to include the SUBJECT PERSON and any backpacks, bags, or other containers that SUBJECT PERSON may be carrying, as well as any digital devices(s) or other electronic storage media found on the SUBJECT PERSON or therein.

ATTACHMENT B**ITEMS TO BE SEIZED**

Evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt/Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) committed in or after January 2019:

- a. Items, records, or information³ relating to visual depictions of minors engaged in sexually explicit conduct;
- b. Items, records, or information relating to the use of the Kik Network;
- c. Items, records, or information relating to the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;
- d. Items, records, or information concerning communications about the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;
- e. Items, records, or information concerning communications about the sexual abuse or exploitation of minors;
- f. Items, records, or information related to communications with or about minors;
- g. Items, records, or information concerning the identities and contact information (including mailing addresses) of any individuals involved in the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct, saved in any form;
- h. Items, records, or information concerning occupancy, residency or ownership of the SUBJECT PREMISES, including without limitation,

³ As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

1 utility and telephone bills, mail envelopes, addressed correspondence,
 2 purchase or lease agreements, diaries, statements, identification documents,
 3 address books, telephone directories, and keys;

4 i. Items, records, or information concerning the ownership or use of computer
 5 equipment found in the SUBJECT PREMISES, including, but not limited
 6 to, sales receipts, bills for internet access, handwritten notes, and computer
 7 manuals;

8 j. Any digital devices or other electronic storage media⁴ and/or their
 9 components including:

10 i. any digital device or other electronic storage media capable of being
 11 used to commit, further, or store evidence, fruits, or instrumentalities
 12 of the offenses listed above;

13 ii. any magnetic, electronic or optical storage device capable of storing
 14 data, including thumb drives, SD cards, or external hard drives;

15 iii. any physical keys, encryption devices, dongles and similar physical
 16 items that are necessary to gain access to the computer equipment,
 17 storage devices or data; and

18 iv. any passwords, password files, test keys, encryption codes or other
 19 information necessary to access the computer equipment, storage
 20 devices or data.

21 k. For any digital device or other electronic storage media whose seizure is
 22 otherwise authorized by this warrant, and any digital device or other
 23 electronic storage media that contains or in which is stored records or
 24 information that is otherwise called for by this warrant:

25 i. evidence of who used, owned, or controlled the digital device or
 26 other electronic storage media at the time the things described in this
 27 warrant were created, edited, or deleted, such as logs, registry
 28

26 ⁴ The term “digital devices” includes all types of electronic, magnetic, optical, electrochemical,
 27 or other high speed data processing devices performing logical, arithmetic, or storage functions,
 28 including desktop computers, notebook computers, mobile phones, tablets, server computers, and
 network hardware. The term “electronic storage media” includes any physical object upon
 which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash
 memory, CD-ROMs, and other magnetic or optical media.

1 entries, configuration files, saved usernames and passwords,
2 documents, browsing history, user profiles, email, email contacts,
3 “chat,” instant messaging logs, photographs, and correspondence;

4 ii. evidence of software that would allow others to control the digital
5 device or other electronic storage media, such as viruses, Trojan
6 horses, and other forms of malicious software, as well as evidence of
7 the presence or absence of security software designed to detect
8 malicious software;

9 iii. evidence of the lack of such malicious software;

10 iv. evidence of the attachment to the digital device of other storage
11 devices or similar containers for electronic evidence;

12 v. evidence of counter-forensic programs (and associated data) that are
13 designed to eliminate data from the digital device or other electronic
14 storage media;

15 vi. evidence of the times the digital device or other electronic storage
16 media was used;

17 vii. passwords, encryption keys, and other access devices that may be
18 necessary to access the digital device or other electronic storage
19 media;

20 viii. documentation and manuals that may be necessary to access the
21 digital device or other electronic storage media or to conduct a
22 forensic examination of the digital device or other electronic storage
23 media;

24 ix. records of or information about the Internet Protocol used by the
25 digital device or other electronic storage media;

26 x. records of internet activity, including firewall logs, caches, browser
27 history and cookies, “bookmarked” or “favorite” web pages, search
28 terms that the user entered into any internet search engine, and
records of user-typed web addresses.

xi. contextual information necessary to understand the evidence
described in this attachment.

1 This warrant authorizes a review of electronic storage media and electronically stored
2 information seized or copied pursuant to this warrant in order to locate evidence, fruits,
3 and instrumentalities described in this warrant. The review of this electronic data may be
4 conducted by any government personnel assisting in the investigation, who may include,
5 in addition to law enforcement officers and agents, attorneys for the government, attorney
6 support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a
7 complete copy of the seized or copied electronic data to the custody and control of
8 attorneys for the government and their support staff for their independent review.

9 THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE
10 MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS
11 SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO
12 THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC
13 STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL
14 ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE
15 CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR
16 EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED
17 CRIMES.
18
19
20
21
22
23
24
25
26
27
28